# *Software crash*

- Written in Java; runs in a virtual machine “sandbox” that protects against some classes of programming errors.
- If display program crashes, there is no effect on control program.
- If control program crashes, current motion is safe: each step is pre-approved before the motion command is issued.
- Either program can simply be restarted if necessary:
  - Encoder readings are retained in hardware.
  - Calibrations, geometry, etc. are read from log file when program starts.

# *Power failure*

- Encoder absolute positions reset to zero.
- Partial power failure will result in immediate stop because of readout anomaly or sensor disagreement.
- Log files are retained.
- Potential procedure:
  - Check log file for last-known reading from encoder.
  - Compare against position from pressure transducers and possible LED run.
  - Reset calibration of encoder to match physical value.
  - Withdraw pole to vertical position and begin again.

# *Failure of a single motor*

- Scenario: motion requested on both axes simultaneously, but only occurs on one axis.
- Could result in tilting the pole to an angle rather than simply moving vertically.
- Either:
  - Step must be pre-approved with each cable moving independently, OR
  - “Deadman timer” must be set to stop motion if computer monitoring does not occur at least of order 0.1 s. Computer can trigger an immediate stop in case of problems.